UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER OF PATENTS AND TRADEMARKS
Washington, D.C. 20231
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/429,624	10/29/1999	MARCEL M. YUNG	10624.0015	6146

7590 10/17/2002

STUART T F HUANG
STEPTOE & JOHNSON LLP
1330 CONNECTICUT AVENUE NW
WASHINGTON, DC 200361795

EXAMINER
SONG, HOSUK

ART UNIT	PAPER NUMBER
2131	

DATE MAILED: 10/17/2002

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary

Application No.	Applicant(s)
09/429,624	YUNG ET AL.
Examiner	**Art Unit**
HO S. SONG	2131

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136 (a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1) ☒ Responsive to communication(s) filed on *Aug 9, 2002* .

2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.

3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11; 453 O.G. 213.

Disposition of Claims

4) ☒ Claim(s) *1-31* is/are pending in the application.

4a) Of the above, claim(s) _____ is/are withdrawn from consideration.

5) ☐ Claim(s) _____ is/are allowed.

6) ☒ Claim(s) *1-31* is/are rejected.

7) ☐ Claim(s) _____ is/are objected to.

8) ☐ Claims _____ are subject to restriction and/or election requirement.

Application Papers

9) ☐ The specification is objected to by the Examiner.

10) ☐ The drawing(s) filed on _____ is/are a) ☐ accepted or b) ☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

11) ☐ The proposed drawing correction filed on _____ is: a) ☐ approved b) ☐ disapproved by the Examiner.

If approved, corrected drawings are required in reply to this Office action.

12) ☐ The oath or declaration is objected to by the Examiner.

Priority under 35 U.S.C. §§ 119 and 120

13) ☐ Acknowledgement is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a) ☐ All b) ☐ Some* c) ☐ None of:

1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. _____ .
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

*See the attached detailed Office action for a list of the certified copies not received.

14) ☐ Acknowledgement is made of a claim for domestic priority under 35 U.S.C. § 119(e).

a) ☐ The translation of the foreign language provisional application has been received.

15) ☐ Acknowledgement is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449) Paper No(s). _____
4) ☐ Interview Summary (PTO-413) Paper No(s). _____
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other:

DETAILED ACTION

Claim Rejections - 35 USC § 102

(a) the invention was known or used by others in this country, or patented or described in a printed publication in this or a foreign country, before the invention thereof by the applicant for a patent.

(e) the invention was described in a patent granted on an application for patent by another filed in the United States before the invention thereof by the applicant for patent, or on an international application by another who has fulfilled the requirements of paragraphs (1), (2), and (4) of section 371© of this title before the invention thereof by the applicant for patent.

1. Claims 1-11 remain rejected under 35 U.S.C. 102(a) as being anticipated by Gennaro et al.(Robust Threshold DSS Signatures).

In claim 1, Gennaro disclose computing shared values over a known and agreed context, each value being known by each member of a distinct subset of the plurality of distributed electronic devices and at each of a plurality of the distributed electronic devices, generating a random value using said shared values in (pages 351-356 and 362-363). Gennaro disclose at each of a plurality of the distributed electronic devices, generating a partial result for the distributed cryptographic computation using at least one of random values and computing a final result for the distributed cryptographic computation using partial results in (page 365).

In claim 2, Gennaro discloses the method of distributed cryptographic computation as recited by claim 1, wherein shared values are random keys in (pages 361-368).

In claim 3, Gennaro discloses the method of distributed cryptographic computation as recited by claim 1, wherein shared values are derived from a cryptographic protocol in (page 365).

In claim 4, Gennaro discloses the method of distributed cryptographic computation as recited by claim 1, wherein shared values are derived cryptographically in (page 361-368).

In claim 5, Gennaro discloses the method of distributed cryptographic computation as recited by claim 1, comprising the step of implementing a re-representation of a function in (page 362).

In claim 6, Gennaro discloses the method of distributed cryptographic computation as recited by claim 1, wherein said partial results may include incorrect values in (page 354 and 364).

In claim 7, Gennaro discloses the method of distributed cryptographic computation as recited by claim 1, wherein steps of claim 1 are performed iteratively in (page 365).

In claim 8, Gennaro discloses the method of distributed cryptographic computation as recited by claim 7, comprising changing shared values after step of generating an output based on partial result in (pages 355-356).

In claim 9, Gennaro discloses the method of distributed cryptographic computation as recited by claim 3, wherein cryptographic protocol is a cryptographic function involving exponentiation in (pages 356 and 365).

In claim 10, Gennaro discloses the method of distributed cryptographic computation as recited by claim 3, wherein cryptographic protocol is an RSA function in (pages 356 and 365).

In claim 11, it is inherent to have a hardware/computing device in Gennaro to store data in order to carry out a cryptographic computation.

2. Claims 1-4 and 9-12,17-31 remain rejected under 35 U.S.C. 102(e) as being anticipated by Brickell(US 5,867,578).

In claim 1, Brickell disclose computing shared values over a known and agreed context, each value being shared among a distinct subset of the plurality of distributed electronic devices and at each of a plurality of the distributed electronic devices, generating a random value using said shared values in (col.3, lines 66-67, col.4, lines 1-20). Brickell disclose at each of a plurality of the distributed electronic devices, generating a partial result for the distributed cryptographic computation using at least one of random values and computing a final result for the distributed cryptographic computation using partial results in (col.9, line 10-col.10, line 31,col.11, lines 10-65).

In claim 2, Brickell discloses the method of distributed cryptographic computation as recited by claim 1, wherein shared values are random keys in (col.9, lines 34-46).

In claim 3, Brickell discloses the method of distributed cryptographic computation as recited by claim 1, wherein shared values are derived from a cryptographic protocol in (col.9, lines 10-65,col.10, lines 1-10).

In claim 4, Brickell discloses the method of distributed cryptographic computation as recited by claim 1, wherein shared values are derived cryptographically in (col.9, lines 10-65,col.10, lines 1-10).

In claim 9, Brickell discloses the method of distributed cryptographic computation as recited by claim 3, wherein cryptographic protocol is a cryptographic function involving exponentiation in (col.9, line 10-col.10, line 31).

In claim 10, Brickell discloses the method of distributed cryptographic computation as recited by claim 3, wherein cryptographic protocol is an RSA function in (col.10, lines 52-53).

In claim 11, Brickell discloses the method of distributed cryptographic computation as recited by claim 1, wherein shared values are stored in a hardware device in at least one of distributed electronic devices in (col.7, lines 49-67, col.8, lines 1-14).

In claim 12, Brickell discloses selecting a subgroup of devices to perform the distributed cryptographic communication and computing shared values over a known and agreed context, each value being shared among a distinct subset of he subgroup of distributed electronic devices in (fig.1, col.14, lines 9-64). Brickell discloses generating a random value using shared values at each distributed electronic devices and generating a partial result for the cryptographic computation using a share of the cryptographic value and at least one of random values and computing a final result for the distributed cryptographic computation using partial results in (col.3, lines 66-67, col.4, lines 1-20; col.9, line 10-col.10, line 31,col.11, lines 10-65).

In claims 17-22, Brickell discloses the computed shared value is shared among a subset of the distributed electronic devices in (fig.1, col.14, lines 29-67).

In claim 23, Brickell disclose wherein the random values depend upon the particular set of devices selected for the subgroup in (fig.1 and col.9, lines 11-30).

In claim 24, Brickell disclose cryptographic computation is based on an argument, and generated random values are based on an argument in (col.9, lines 10-65,col.10, lines 1-10).

In claim 25, distributed cryptographic computation as recited by claim 12 wherein the cryptographic computation is based on an argument, and the generated random values are based on said argument in (col.3, lines 66-67, col.4, lines 1-20; col.9, line 10-col.10, line 31,col.11, lines 10-65).

In claim 26, Brickell disclose wherein the cryptographic computation comprises digital signing in (col.9, line 10-col.10, line 31,col.11, lines 10-65).

In claim 27, Brickell disclose cryptographic computation as recited by claim 12 wherein the cryptographic computation comprises digital signing in (col.3, lines 66-67, col.4, lines 1-20; col.9, line 10-col.10, line 31,col.11, lines 10-65).

In claims 28-29, Brickell discloses step of using generated random values or shared values to detect misbehaving devices in (col.14, lines 9-28).

In claims 30-31, Brickell discloses proactively updating a secret cryptographic value used in the cryptographic computation in (col.23, lines 65-col.24, lines 1-10).

Response to Applicant's Arguments

3. Applicant has amended Claim 1.

4. The rejections of the previous action are maintained.

5. Applicant's arguments filed 8/09/02 have been fully considered but they are not persuasive.

Applicant has argued that Gennaro does not disclose such a sharing of sources of randomness for use in computing and sharing of Gennaro is the sharing of a secret key in the form of values related to but different from the key. Applicant further argues that none of the group members individually possesses sufficient information to know the key. ***In response***: the examiner disagree. Gennaro discloses that secret random value is jointly generated and shared by the members using Feldman's VSS protocol (see page 364) and Gennaro in page 360 teaches defining or deriving a secret value or key using the shared values. ***Applicant has argued that*** shared value of the embodiment of Fig.1 of applicant's invention is used to index a pseudo random function to generate values useful for detecting misbehaving members of the group and Gennarois silent on these features. ***In response:*** please point out in the claim where applicant is claiming such a feature where shared values are used to index a pseudo random function to generate values useful for detecting misbehaving members of the group.

Conclusion

6 **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period

will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Information Regarding Communication with the PTO

7. Any inquiry concerning this communication or earlier communication from the examiner should be directed to Ho S. Song whose telephone number is (703)305-0042. The examiner can normally be reached on Tuesday-Friday from 6:00 am - 4:00 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gail Hayes, can be reached on (703)305-9711.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the Group receptionist whose telephone number is (703)305-3900.

Ho Song

Gail Hayes

GAIL HAYES
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100